(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
7. Oktober 2004 (07.10.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/086220 A3

(51) Internationale Patentklassifikation[7]: G06F 11/14, G07F 7/10, G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2004/003004

(22) Internationales Anmeldedatum:
22. März 2004 (22.03.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 13 318.6 25. März 2003 (25.03.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **STOCKER, Thomas** [DE/DE]; Königseestrasse 48a, 81825 München (DE).

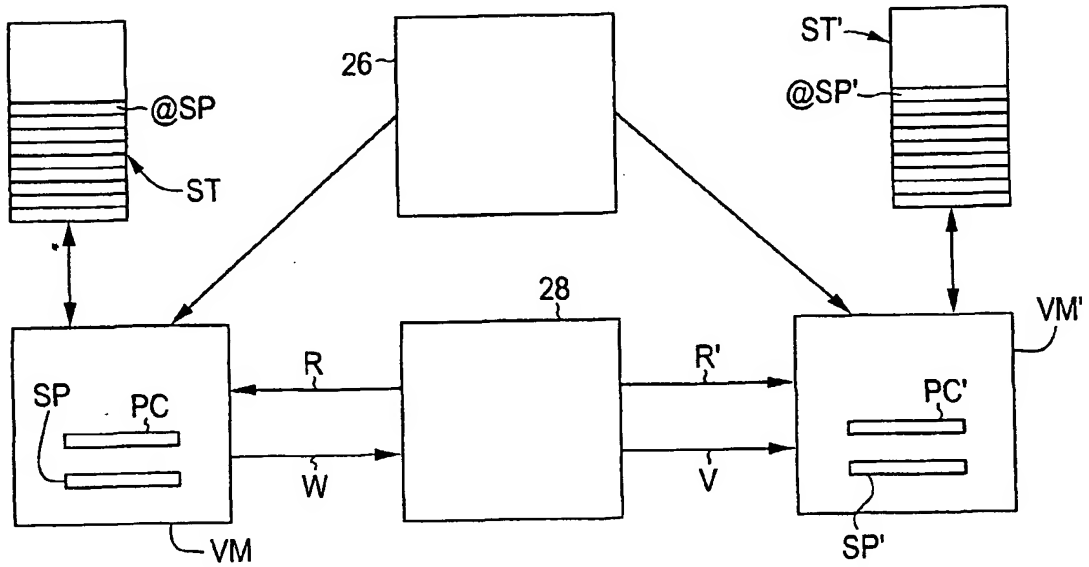
(74) Anwalt: **DENDORFER, Claus**; Wächtershäuser & Hartz, Weinstrasse 8, 80333 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: CONTROLLED EXECUTION OF A PROGRAM USED FOR A VIRTUAL MACHINE ON A PORTABLE DATA CARRIER

(54) Bezeichnung: KONTROLLIERTE AUSFÜHRUNG EINES FÜR EINE VIRTUELLE MASCHINE VORGESEHENEN PROGRAMMS AUF EINEM TRAGBAREN DATENTRÄGER



(57) Abstract: Disclosed is a method for the controlled execution of a program (26) used for a virtual machine (VM, VM') on a portable data carrier that comprises a processor executing at least one first and a second virtual machine (VM, VM'). According to the inventive method, the program (26) is executed by both the first and the second virtual machine (VM, VM'). Execution of the program is aborted in case a deviation of the mode of operation of the first virtual machine (VM) from the mode of operation of the second virtual machine (VM') is detected during execution of the program (26). A data carrier and a computer program are provided with corresponding characteristics. The invention creates technology for controlled program execution, which prevents safety hazards due to an attack or malfunction of the data carrier.

[Fortsetzung auf der nächsten Seite]

WO 2004/086220 A3

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärung gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO Patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) **Veröffentlichungsdatum des internationalen Recherchenberichts:** 28. April 2005

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) **Zusammenfassung:** Bei einem Verfahren zur kontrollierten Ausführung eines für eine virtuelle Maschine (VM, VM') vorgesehenen Programms (26) auf einem tragbaren Datenträger, wobei der Datenträger einen Prozessor aufweist, der mindestens eine erste und eine zweite virtuelle Maschine (VM, VM') ausführt, wird das Programm (26) sowohl von der ersten als auch von der zweiten virtuel len Maschine (VM, VM') ausgeführt. Falls während der Ausführung des Programms (26) eine Abweichung des Betriebszustands der ersten virtuellen Maschine (VM) von dem Betriebszustand der zweiten virtuellen Maschine (VM') festgestellt wird, wird die Programmausführung abgebrochen. Ein Datenträger und ein Computerprogrammprodukt weisen entsprechende Merkmale auf. Die Erfindung stellt eine Technik zur kontrollierten Pro grammausführung bereit, die Sicherheitsrisiken durch einen Angriff oder eine Betriebsstörung des Datenträgers vermeidet.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/003004

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/14 G07F7/10 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, IBM-TDB, INSPEC, COMPENDEX, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 271 317 A (NAGRACARD S.A) 2 January 2003 (2003-01-02) paragraphs '0001! - '0017!, '0020!, '0036! - '0038! claims 1,17,18 -----	1-6,9-11
Y	THANH NGUYEN: COTS JOURNAL, 'Online! December 2001 (2001-12), pages 14-20, XP002317390 Retrieved from the Internet: URL:http://www.rtcgroup.com/cotsjournal/pdfs/2001/12/cots12-ruggedside.pdf> 'retrieved on 2005-02-11! page 14, middle column, lines 5-8 page 14, right-hand column, lines 4-12 page 18, right-hand column, lines 3-35; figure 4 ----- -/--	1-6,9-11

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 February 2005	02/03/2005
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Lanchès, P

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ROTENBERG E ED - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: "AR-SMT: A MICROARCHITECTURAL APPROACH TO FAULT TOLERANCE IN MICROPROCESSORS" 29TH ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING. DIGEST OF PAPERS. (FTCS-29). MADISON, WI, JUNE 15 - 18, 1999, ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING, LOS ALMITOS, CA : IEEE COMP. SOC, US, 15 June 1999 (1999-06-15), pages 84-91, XP000873029 ISBN: 0-7803-5763-9 page 85, left-hand column, line 1 - page 86, left-hand column, line 20	5
A	US 5 488 716 A (SCHNEIDER ET AL) 30 January 1996 (1996-01-30) column 3, line 42 - line 48 column 4, line 48 - line 65 figure 1	1,10,11
A	GB 2 353 113 A (* SUN MICROSYSTEMS, INC) 14 February 2001 (2001-02-14) cited in the application abstract	1,10,11

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Inter[redacted]nal Application No
PCT/EP2004/003004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1271317 A	02-01-2003	EP 1271317 A1	02-01-2003
US 5488716 A	30-01-1996	WO 9309494 A1	13-05-1993
GB 2353113 A	14-02-2001	US 6625751 B1	23-09-2003

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/003004

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F11/14 G07F7/10 G06F1/00

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, IBM-TDB, INSPEC, COMPENDEX, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 1 271 317 A (NAGRACARD S.A) 2. Januar 2003 (2003-01-02) Absätze '0001! - '0017!, '0020!, '0036! - '0038! Ansprüche 1,17,18 -----	1-6,9-11
Y	THANH NGUYEN: COTS JOURNAL, 'Online! Dezember 2001 (2001-12), Seiten 14-20, XP002317390 Gefunden im Internet: URL:http://www.rtcgroup.com/cotsjournal/pdfs/2001/12/cots12-ruggedside.pdf> 'gefunden am 2005-02-11! Seite 14, mittlere Spalte, Zeilen 5-8 Seite 14, rechte Spalte, Zeilen 4-12 Seite 18, rechte Spalte, Zeilen 3-35; Abbildung 4 -----	1-6,9-11
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. Februar 2005	02/03/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Lanchès, P

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	ROTENBERG E ED - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: "AR-SMT: A MICROARCHITECTURAL APPROACH TO FAULT TOLERANCE IN MICROPROCESSORS" 29TH ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING. DIGEST OF PAPERS. (FTCS-29). MADISON, WI, JUNE 15 - 18, 1999, ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING, LOS ALMITOS, CA : IEEE COMP. SOC, US, 15. Juni 1999 (1999-06-15), Seiten 84-91, XP000873029 ISBN: 0-7803-5763-9 Seite 85, linke Spalte, Zeile 1 - Seite 86, linke Spalte, Zeile 20	5
A	US 5 488 716 A (SCHNEIDER ET AL) 30. Januar 1996 (1996-01-30) Spalte 3, Zeile 42 - Zeile 48 Spalte 4, Zeile 48 - Zeile 65 Abbildung 1	1,10,11
A	GB 2 353 113 A (* SUN MICROSYSTEMS, INC) 14. Februar 2001 (2001-02-14) in der Anmeldung erwähnt Zusammenfassung	1,10,11

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 1271317	A	02-01-2003	EP	1271317 A1	02-01-2003
US 5488716	A	30-01-1996	WO	9309494 A1	13-05-1993
GB 2353113	A	14-02-2001	US	6625751 B1	23-09-2003